## REMARKS

Reconsideration of this application, as amended, is respectfully requested.

Claims 1-4, 6, and 8-37 have been rejected.

In this response, claims 1, 21, and 37 have been amended. No claims have been canceled. No claims have been added. Support for the amendments is found in the specification, the drawings, and in the claims as originally filed. Applicants submit that the amendments do not add new matter.

Applicants reserve all rights with respect to the applicability of the Doctrine of Equivalents.

Please enter the following response to the Interview Summary mailed August 30, 2010. The undersigned representative for applicants thanks the Examiner for the courtesy of a telephonic interview on August 25, 2010. Applicants agree with the Examiner and the summary of the telephonic interview of August 25, 2010, regarding the proposed claim changes which were carried out by the present Amendment.

Claims 1-37 stand rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,374,077 to Shimura ("Shimura") and further in view of U.S. Patent No. 7,080,098 to Smirniotopoulos ("Smirniotopoulos") and further in view of U.S. Publication No. 2004/0139043 to Lei et al. ("Lei").

Amended claim 1 reads as follows:

> A method for retrieving medical images from various sources and in different formats, to enable the creation of teaching files and research datasets, for the building of a personal medical image library, the method comprising:
> (a) directly retrieving a plurality of medical images from various sources;
> (b) storing the plurality of medical images in a database;
> (c) generating a database record for the teaching files and research datasets;
> (d) generating the teaching files and research datasets using at least one medical image of the plurality of medical images and additional information input by a user, the

teaching files and research datasets being compliant with at least one predetermined schema;

(e) saving the teaching files and research datasets into the database;

(f) generating at least one index of the teaching files and research datasets;

(g) automatically anonymizing patient identification data when the at least one medical image is retrieved from the various sources, wherein the patient identification data comprises patient sensitive information that is not revealed publicly, wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code; and

(h) securely storing a relationship between the anonymization code and the patient identification data in a table in the database.

(Amended claim 1)(emphasis added)

Support for the amendment to claim 1 including "securely storing a relationship between the anonymization code and the patient identification data in a table in the database" can be found in Figure 4 (operation 47) and paragraphs [0155] and [0156] of the publication of the present US patent application.

Amended claim 1 requires saving the teaching files and research datasets into the database and automatically anonymizing sensitive information by replacing each item of the patient identification data with an anonymization code and securely storing a relationship between the anonymization code and the patient identification data in a table in the database. That is, the teaching files and research datasets in the database do not contain any confidential data and are easily directly accessible. Automatically anonymizing the sensitive information by replacing each item of the sensitive information with an anonymization code and securely storing a relationship between the anonymization code and the sensitive information in a table in the database results in a simplified access control scheme for the largest portion of the database (which is particularly useful in a large distributed database). This saves a lot of computational resources, in particular, for a large database where otherwise a large number of queries need to be processed. Additionally, securely storing a relationship between the anonymization code and the

patient identification data in a table in the database "centralizes" the sensitive information in a small core table that can be relatively easily secured.

The Examiner acknowledged that "Shimura and Smirniotopoulos do not explicitly disclose: wherein the automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code." (Office Action, p. 5)

Accordingly, a combination of Shimura and Smirniotopoulos fails to disclose automatically anonymizing patient identification data by replacing each item of the patient identification data with an anonymization code and securely storing a relationship between the anonymization code and the patient identification data in a table in the database, as recited in amended claim 1.

Lei, in contrast, discloses attribute relevant access control policies. More specifically, Lei discloses a database system which provides the feature of an implementation of a user-defined policy with respect to the provision of confidential data. In particular, Lei discloses the following:

> Policy function 232 may be designed, for example, to read user-supplied policy metadata and behave based on the content of the metadata. ... For the purpose of explanation, an embodiment shall be described in which policy function 232 is designed to determine if and how the query 221 should be modified. According to one embodiment, if policy function 232 determines that query 221 should be modified, then policy function 232 returns a predicate that is appended to query 221 to create a modified query."
>
> For example, assuming the user 210 is "John" and that "SALARY" is a restricted attribute of table t2, when semantic analyzer 231 determines that query 221 attempts to access data from the "SALARY" attribute, semantic analyzer 231 may invoke policy function 232. Policy function 232 may be implemented in such a way as to only allow "John" to access his own salary. In this case, the policy function 232 may return a predicate that is appended to query 221 in order to ensure that the query only retrieves row 113, thus allowing John to see only his own salary, as will be described in more detail.
>
> According to one embodiment, the attribute restriction metadata 243 indicates what values (referred to hereinafter as "masking values") may be

> used to mask data from restricted attributes. For example, assuming that "SALARY" is a restricted attribute, if John attempts to access names and salaries for all rows in table t2, John will receive the names from all of the rows but the data from the salary column may be masked with a masking value, such as an integer zero. In this case, when John requests the names and salaries for all of the rows in table t2, the database server 230 retrieves all of the names and salaries from table t2 and stores the unmodified names and salaries in result set 235. The semantic analyzer 231 determines that John is attempting to access a restricted attribute, "SALARY". The result set 235 is passed to the masking routine 234 which uses the specified masking value, integer zero, to mask the restricted attribute "SALARY", thus creating the masked result set 233. The masked result set 233 is provided to the database application 220.

(Lei, paragraphs [0029]-[0031]) (emphasis added)

As set forth above, Lei discloses that the semantic analyzer 231 analyzes every query that the database server receives. More specifically, Lei discloses that if the semantic analyzer 231 determines that the query attempts to access one or more restricted attributes, the policy function 232 changes the query (paragraph [0029]). This technique requires a lot of computational resources because every query has to be analyzed. Further, Lei discloses that the database records in each table include the non-sensitive information ("names") and the sensitive information ("salary") (paragraph [0030]). As set forth above, Lei discloses that the masking routine is carried out on the result set 235, which represents the unmodified query result provided by the database. Thus, the result set 235 still includes the non-sensitive information and the sensitive information (Figure 2, paragraph [0031]). Only the result set 235 is masked to provide the masked result set 233, which is finally output to the database application and eventually to the user (Figure 2). In Lei, because all the database records include non-sensitive information and the sensitive information all database records are protected against unauthorized access.

In contrast, amended claim 1 refers to securely storing a relationship between the anonymization code and the patient identification data in a table in the database. Lei fails to

disclose automatically anonymizing patient identification data that includes replacing each item of the patient identification data with an anonymization code and securely storing a relationship between the anonymization code and the patient identification data in a table in the database, as recited in amended claim 1.

It is respectfully submitted that none of the references cited by the Examiner teach or suggest a combination with each other. Lei teaches attribute relevant access control policies. Smirniotopoulos, in contrast, teaches medical multimedia database system. Shimura, in contrast, teaches similar image search system. It would be impermissible hindsight, based on applicants' own disclosure, to combine Lei, Smirniotopoulos, and Shimura.

Furthermore, even if the access control policies of Lei, multimedia database system of Smirniotopoulos, and similar image search system of Shimura were combined, such a combination would still lack automatically anonymizing patient identification data that includes replacing each item of the patient identification data with an anonymization code and securely storing a relationship between the anonymization code and the patient identification data in a table in the database, as recited in amended claim 1.

Therefore, applicants respectfully submit that claim 1, as amended, is not obvious under 35 U.S.C. §103(a) over Shimura, Smirniotopoulos, and Lei.

Given that amended independent claims 21 and 37 contain limitations that are similar to those limitations set forth above, applicants respectfully submit that claims 21 and 37, as amended, are not obvious under 35 U.S.C. §103(a) over Shimura, Smirniotopoulos, and Lei.

Given that claims 2-20, and 22-36 depend from amended claims 1 or 21 respectively, and add additional limitations, applicants respectfully submit that claims 2-20, and 22-36 are not obvious under 35 U.S.C. §103(a) over Shimura, Smirniotopoulos, and Lei.

Claims 24-28 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Shimura and further in view of U.S. Publication No. 2003/0013951 to Stefanescu ("Stefanescu").

Applicants do not admit that Stefanescu is prior art and reserve the right to swear behind Stefanescu at a later date.

As set forth above, even if Lei, Smirniotopoulos, Shimura were combined, such a combination would still lack the limitation of automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code and securely storing a relationship between the anonymization code and the patient identification data is stored securely in a table in the database, as recited in amended claim 21.

Stefanescu, in contrast, discloses organizing and searching database of medical images. Stefanescu fails to disclose an MIRC server configured to automatically anonymize patient identification data that includes replacing each item of the patient identification data with an anonymization code, wherein a relationship between the anonymization code and the patient identification data is stored securely in a table in the database, as recited in amended claim 21.

It is respectfully submitted that none of the references cited by the Examiner teach or suggest a combination with each other. It would be impermissible hindsight, based on applicants' own disclosure to combine Stefanescu, Lei, Shimura, and Smirniotopoulos.

Furthermore, even if the database organization and searching of Stefanescu, medical multimedia database system of Smirniotopoulos, and the access control policies of Lei were incorporated into the image search system of Shimura, such a combination would still lack the limitation of automatic anonymizing of patient identification data includes replacing each item of the patient identification data with an anonymization code, wherein a relationship between the anonymization code and the patient identification data is stored securely in a table in the database, as recited in amended claim 21.

Given that claims 24-28 depend from amended claim 21, and add additional limitations, applicants respectfully submit that claims 24-28 are not obvious under 35 U.S.C. §103(a) over Shimura in view of Smirniotopoulos.

It is respectfully submitted that in view of the amendments and arguments set forth herein, the applicable rejections and objections have been overcome. If the Examiner believes a telephone conference would assist in the prosecution of the present application, the Examiner is invited to call the undersigned.

If there are any additional charges, please charge Deposit Account No. 02-2666 for any fee deficiency that may be due.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: September 23, 2010

Tatiana Rossin/

Tatiana Rossin
Reg. No.: 56,833

1279 Oakmead Parkway
Sunnyvale, California 94085-4040
(408) 720-8300

Customer No. 087901